Supreme Court, U.S.
FILED
10-303 AUG 25 2010
OFFICE OF THE CLERK

No. 10

IN THE SUPREME COURT OF THE UNITED STATES

PETER JOHN LAMANA,

Petitioner,

v.

COMMONWEALTH OF PENNSYLVANIA,

Respondent.

Petition for Writ of Certiorari
To the Superior Court of Pennsylvania

PETITION FOR WRIT OF CERTIORARI

MARC NEFF
13th Floor
1818 Market Street
Philadelphia, PA 19103
(215) 563-9800

PETER GOLDBERGER
Counsel of Record
PAMELA A. WILK
50 Rittenhouse Pl.
Ardmore, PA 19003
(610) 649-8200
Attorneys for Petitioner

August 2010

QUESTIONS PRESENTED

A public employee's personal computer, kept at work, was seized under a warrant. Evidence discovered in a forensic search of that computer underlies the conviction. The warrant was obtained on the basis of information learned in a prior warrantless examination of the computer's files by a police officer, which followed a search of those files by the employer.

1. Despite taking his personal computer to work and using it there, does a public employee retain a constitutionally protected "expectation of privacy" in files stored on that computer, as against both the employer and the police?

2. Did the warrantless police examination of a teacher's personal computer, in the classroom, violate the Fourth Amendment, where the police acted at the request of and upon information provided by the school district, his employer?

3. Is a workplace search of a teacher's personal computer permissible under the Fourth Amendment (a) simply because a similar search might be regarded as "reasonable and normal in the private-employer context," per O'Connor v. Ortega, 480 U.S. 709, 731 (1987) (Scalia, J., concurring); or (b) only if (i) motivated by a non-investigatory work-related purpose, (ii) there were "reasonable grounds for suspecting the search was necessary to achieve" that purpose, and (iii) reasonable in scope (see id. at 726 (plurality opinion))?

LIST OF ALL PARTIES

The caption of the case in this Court contains the names of all parties (Peter John Lamana and the Commonwealth of Pennsylvania). Mr. Lamana had no co-defendants.

TABLE OF CONTENTS

QUESTIONS PRESENTED i
LIST OF ALL PARTIES ii
INDEX TO APPENDIX iv
TABLE OF AUTHORITIES v

PETITION
OPINIONS BELOW 1
JURISDICTION 2
CONSTITUTIONAL PROVISIONS INVOLVED 2
STATEMENT OF THE CASE
a. Procedural History 3
b. Statement of Facts 5
c. Raising and Resolution of Federal Question in State Courts 10
REASONS FOR GRANTING THE WRIT 16
The relatively simple facts of this case make it a suitable vehicle for the Court to address the important issues it has twice granted certiorari to resolve: How does the Fourth Amendment apply to a public employer's workplace search of an employee's private property or information, which in turn leads to a warrantless law enforcement search and a criminal prosecution? 17
a. Expectation of privacy 23
b. What is the correct reasonableness test? 25
c. Initial warrantless police examination 30

CONCLUSION 33

INDEX TO APPENDIX

A. Memorandum Opinion (not precedential) of the Superior Court of Pennsylvania (Nov. 23, 2009) ..... App. A1

B. Post-Trial opinion of the Court of Common Pleas of Berks County, Pa., 7 Pa.D.&C.5th 225 (Feb. 2, 2009) ..... App. B1

C. Findings of Fact and Conclusions of Law, and Order, on motion to suppress (C.P. Berks Co., Pa., Jan. 10, 2007) ..... App. C1

D. Order of the Supreme Court of Pennsylvania denying petition for allowance of appeal (May 27, 2010) ..... App. D1

TABLE OF AUTHORITIES

CASES

City of Indianapolis v. Edmond,
531 U.S. 32 (2000) 27
City of Ontario v. Quon, 558 U.S. --,
130 S.Ct. 1011 (2009) (No. 08-1332) 18
City of Ontario v. Quon, 560 U.S. --,
130 S.Ct. 2619 (2010) 18, 19, 23, 25-28, 33
Ferguson v. City of Charleston, 532 U.S. 67 (2001) 31
Frazier v. Cupp, 394 U.S. 731 (1969) 31
Georgia v. Randolph, 547 U.S. 103 (2006) 31
Illinois v. Rodriguez, 497 U.S. 177 (1990) 31
Kyllo v. United States, 533 U.S. 27 (2001) 23
Mancusi v. DeForte, 392 U.S. 364 (1968) 23
Murray v. United States, 487 U.S. 533, 543 (1988) 22
National Treas. Employees Union v. Von Raab,
489 U.S. 656 (1989) 18
O'Connor v. Ortega,
480 U.S. 709 (1987) 17-19, 22, 23, 25-30
Skinner v. Railway Labor Exec. Ass'n,
489 U.S. 602 (1989) 18, 24
United States v. Matlock, 415 U.S. 164 (1974) 31
Walter v. United States, 447 U.S. 649 (1980) 31

CONSTITUTION, STATUTES AND RULES

U.S. Const., amend. IV 2, 18, 23, 30, 32
U.S. Const., amend. XIV, § 1 2
28 U.S.C. § 1257(a) 2
28 U.S.C. § 2101(d) 2
18 Pa.Cons.Stat. § 5903(a) 3
18 Pa.Cons.Stat. § 6312(d) 3

Pa.R.App.P. 1925 4
S.Ct. Rule 13.1 2
S.Ct. Rule 14.1(g) 10
S.Ct. Rule 30.1 2

MISCELLANEOUS

Peter Goldberger, Consent, Expectations of Privacy, and the Meaning of "Searches" in the Fourth Amendment, 75 J.Crim.L. & Crimin. 319 (1984) 23

PETITION FOR WRIT OF CERTIORARI TO THE SUPERIOR COURT OF PENNSYLVANIA

PETER JOHN LAMANA respectfully petitions this Court for a writ of certiorari to review the judgment and opinion of the Superior Court of Pennsylvania filed on November 23, 2009, as to which a petition for allowance of appeal was denied by the state Supreme Court on May 27, 2010.

OPINIONS BELOW

The memorandum opinion of the Superior Court of Pennsylvania (per curiam) was filed on November 23, 2009. A copy is Appendix A; it is noted (but the text is not published) at 988 A.2d 723 (table). The appellate decision adopts the published post-trial memorandum opinion of the Court of Common Pleas for Berks County, Pennsylvania (Parisi, J.) filed on February 2, 2009. Appendix B; Commonwealth v. Lamana, 7 Pa. D.&C.5th 225, 2009 WL 1514617. The trial court also filed an Order with Findings of Fact and Conclusions of Law on January 10, 2007, explaining its denial of petitioner's pretrial motion to suppress. This memorandum is not published; a copy is Appx. C.

JURISDICTION

On May 27, 2010, the Supreme Court of Pennsylvania denied petitioner Lamana's Petition for Allowance of Appeal seeking review of the Superior Court's judgment and memorandum. Appx. D. The instant petition is timely filed within 90 days thereof, or on the first business day thereafter. Rules 13.1, 30.1; 28 U.S.C. § 2101(d). Petitioner invokes this Court's jurisdiction under 28 U.S.C. § 1257(a).

CONSTITUTIONAL PROVISIONS INVOLVED

The **Constitution of the United States** provides, in pertinent part:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const., amend. IV.

> No State shall ... deprive any person of life, liberty, or property, without due process of law; ....

U.S. Const., amend. XIV, § 1.

STATEMENT OF THE CASE

Petitioner Peter J. Lamana stands convicted, following a jury trial in the Court of Common Pleas, Berks County, Pennsylvania, of a single count of possession of child pornography on a personal computer that he kept at his workplace, a public school. The jury acquitted him on one other count.

a. Procedural History

Petitioner, a high school teacher, was arrested on April 1, 2005, on the basis of a criminal complaint which charged offenses allegedly committed on November 29, 2004. The complaint contained nine counts of "sexual abuse of children" by possession of child pornography, in violation 18 Pa.Cons.Stat. § 6312(d), and nine parallel counts of obscenity, id. § 5903(a)(3). The Commonwealth amended the complaint at the preliminary hearing (Aug. 15, 2005) to allege only two counts under § 6312(d) -- one charging possession of nine computerized photographs, and one charging possession of a video. Following the hearing, petitioner was held for court. A formal information charging these two counts was filed September 6, 2005.

On April 3, 2006, in accordance with Pennsylvania procedure, petitioner filed an "omnibus pretrial motion," which included a motion to suppress physical evidence. Specifically, the motion sought suppression of all evidence derived from a warrantless search of his personal computer by the school district's "information technology director" and by a

township police officer. Following a hearing in August 2006, this motion was denied by written Findings and Conclusions on January 10, 2007. Appx. C.[1]

Following a three-day trial in May 2008, the jury convicted petitioner on Count Two (involving a video found on his computer following the challenged search) and acquitted him on Count One (involving digital images). Tr. 5/8/08, at 273. On October 14, 2008, the trial court imposed a sentence of 4 to 23 months' imprisonment, to be followed by five years' probation. The trial court granted petitioner bail pending appeal.

Petitioner filed a timely notice of appeal to the Superior Court of Pennsylvania. In accordance with state appellate procedure, Pa.R.App.P. 1925, petitioner submitted his proposed issues to the trial court, which then filed on February 2, 2009, an opinion in support of its challenged rulings. Appx. B. Following briefing and argument, the Superior Court on November 23, 2009, affirmed petitioner's conviction and sentence in a non-precedential Memorandum. Appx. A. On the suppression issue, the appellate court adopted the opinion of the trial court. Appx. A5. Petitioner's timely application to the Supreme Court of Pennsylvania for allowance of

---

[1] The Order is dated "January 12" above the judge's signature, Appx. C5, but the clerk's file stamp clearly reads "'07 JAN 10." Appx. C1.

appeal was denied by Order filed May 27, 2010. Appx. D. This timely petition for certiorari follows.

b. Statement of Facts

Petitioner Lamana was a teacher at Boyertown High School in Berks County, Pennsylvania. On November 2, 2004, the school district experienced a computer virus attack. The information technology ("IT") department traced the source to a certain data port in Room 802 at the high school.[2] The IT director, Karla Volpi, discovered that petitioner, the teacher assigned to Room 802, had a personally owned computer attached to that port. Citing a district policy against allowing personal computers on the network, Volpi asked petitioner to take his computer home. While it was part of her duties, as the Superintendent of Schools testified, for Volpi "to occasionally inspect computers" used in the schools, Appx. C4 (see Suppr.Tr. 28), she did not see, or ask to see, what was stored on petitioner's computer at that time. She did, however, shut down the port, preventing any computer from accessing the district's network from that spot.[3]

---

[2] The trial court's "Findings of Fact" refer to "classroom 803," Appx. C2, no doubt based on the police officer's recollection at the suppression hearing (Suppr.Tr. 9), but the trial record is clear and uncontradicted that the room in question was 802. "Suppr.Tr." refers to the transcript of the suppression hearing held on August 21, 2006, which was included in the appellate record below.

[3] In October 2004, Volpi had detected an unusual volume

The next day, in connection with petitioner's offer to assist in the virus cleanup effort, Volpi acquiesced in petitioner's request that the port be reopened and that he be allowed to reconnect his computer. Volpi repeated that petitioner would still have to take his computer home, but did not say exactly how soon. Tr. 5/6/08, at 33-34.[4]

On November 19, the school district experienced another virus attack on its network, and again the problem was traced to the same port in Room 802. At that point, Volpi shut down the port permanently. Id. 37-38, 66-67. Nevertheless, further virus activity occurred on November 23 and 24. Volpi did not go to petitioner's classroom or talk to him on November

---

(cont'd)

of data, inconsistent with normal classroom use, being sent from, and especially received by (downloaded to) a certain data port in a classroom at the high school. Tr.(5/6/08), at 25-26. Because of inadequate "mapping" of the ports in the network, however, she was unable to identify precisely the classroom in question at that time. Id. 28. When she went to Room 802 on November 2, she realized that this port had been the source of the high volume of data traffic. Id. 29-30, 32. Petitioner told her that he had installed a popular file-sharing program on his computer, and had been using it to send and receive files through that port, which would be consistent with the volume detected. It could also have been the manner of entry of the virus. Id. 30.

[4] "Tr. 5/6/08" refers to the transcript of the first day of trial, which was also part of the Reproduced Record in the Superior Court.

19, 23 or 24, and no evidence was presented as to whether petitioner had a privately owned computer connected to the network on any of those dates. Id. 38, 67-68. A computer that is not connected to the network is no more of a threat to the district's system than a computer located in a student's or teacher's home. Id. 65-66.

On Monday, November 29, 2004, the schools were still closed for the Thanksgiving holiday; the teachers and students were not present. On that day, Volpi proceeded to Room 802 to investigate whether petitioner's computer was involved in the recent virus attacks.[5] After unlocking the room, she observed a different non-district computer sitting near the suspect data port; however, this computer was turned off and not plugged into any network port. (She later noticed toward the back of the room the computer she had seen on November 2; id. 45.) Volpi powered up the second computer and entered a command to see its directory structure. Id. 41.

Noticing a directory (also called a "folder," that is, a collection of saved files) entitled "shit," Volpi

---

[5] The Superior Court's Memorandum opinion, App. A2, quoting the post-trial opinion, App. B2, mistakenly states, "On November 29, 2004, a virus again attacked the school district's network. Ms. Volpi decided to investigate ...." The record contradicts that recital and instead supports the statement of facts given in text above; there was no new attack on November 29.

decided to investigate its contents.[6] In the folder, she saw a list of thousands of files, id. 77, many with names suggesting sexual activity. Some of these names seemed to refer to children as well. Volpi then opened "one or two" of these files, id. 42, or perhaps three, id. 71, and discovered images of child pornography. She noted that the last access date for these files was November 24, the previous Wednesday. Id. 43. Volpi did not look further to see whether this computer had file-sharing software, nor did she seek to determine whether it was infected with a virus. Id. 81.[7] She turned the computer off and locked the room. Id. 72.

Volpi had her secretary call the principal -- who was out for the day and unavailable -- and the Superintendent of Schools. Id. She urged the Superintendent to meet her "immediately." Suppr.Tr. 29. Volpi then returned to Room 802, took custody of the offending computer, and carried it to the IT office. Id. 73. There, she showed the Superintendent what she had

---

[6] At the preliminary hearing, although not at trial, Volpi testified that she decided to open this folder and investigate its contents because she "thought it[s name] was kind of inappropriate." Tr.(8/15/05), at 5.

[7] Although the personal computer Volpi had observed in petitioner's classroom on November 2 was also present in the room on November 29, id. 45, no testimony was presented to suggest that Volpi also searched that computer.

found. Suppr.Tr. 30-31; Tr. 5/6/08, at 76. He called the local police.[8] At the Superintendent's direction, Volpi then returned petitioner's computer to Room 802. Suppr. Tr. 33-34; see Tr. 5/6/08, at 83-84.

Arriving without a warrant, police officer Evans met Volpi, who told him what she had seen on the computer, Suppr.Tr. 15; Tr. 5/6/08, at 83-84, as did the Superintendent. Suppr.Tr. 36. They went to Room 802, where Volpi again turned on petitioner's computer, this time at the direction of the police officer, Suppr.Tr. 18, 26; Tr. 5/6/08, at 88, and at his direction showed him the offending images she had previously seen. Suppr.Tr. 18; Tr. 5/6/08, at 89-90.[9] The police officer then left, returning later that day, after 4:30 p.m., with a warrant to seize the computer and examine it forensically.

Of "approximately 3688" files in the "shit" directory, id. 151, only ten (nine pictures and one video)

---

[8] School officials in Pennsylvania have an obligation to inform police about any knowledge they have of certain crimes, including abuse of children, occurring in school. Suppr.Tr. 24. The school district and the police department have a "working relationship" in this regard, with which the police "expect and, in fact, demand" that the school district comply. Id.

[9] The Superintendent testified at the suppression hearing that this occurred in the IT office, Suppr.Tr. 35-36, but Volpi and Evans testified at trial (and Evans at the suppression hearing) that it was in the classroom that Volpi showed Evans the offending images.

were alleged to constitute child pornography. Id. 122-23. The forensic examination showed that many of the files in this folder had been opened on November 29 at around 11 a.m., and some at around 2 p.m., and that shortcuts to some of them had been created that morning. Tr. 5/7/08, at 156-61. This scientific evidence contradicted both Ms. Volpi and Officer Evans, who swore they had only looked at two or three files, between 8:00 and 8:30 a.m. and between 12:30 and 1 p.m. respectively.

c. Raising and Resolution of Federal Question in State Courts

Pursuant to this Court's Rule 14.1(g)(i), counsel for the petitioner certifies that the federal questions presented in this petition were raised in the trial court by pretrial motion to suppress, and on appeal. They were ruled upon by the trial court as follows:

> Searches and seizures by government employers or supervisors of the private property of their employees are subject to Fourth Amendment restraints. Commonwealth v. Jackson, 809 A.2d 411, 2002 Pa. Super 311; O'Connor v. Ortega, 480 U.S. 709, 107 S.Ct. 1492. However, the operational realities of the workplace may make some public employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. 480 U.S. at 710. Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis. Id.

In determining the appropriate standard for a search conducted by a public employer in areas in which an employee has a reasonable expectation of privacy, what is a reasonable search depends on the context within which the search takes place, and requires balancing the employee's legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace. Id. Intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this standard, both the inception and the scope of the intrusion must be reasonable. Id.

Here, the initial discovery by Mrs. Volpi was reasonable and there was sufficient probable cause to obtain a search warrant. Mrs. Volpi advised Officer Evans that she came to discover the pornographic images on the Defendant's computer because of her work in connection with a computer virus that has recently affected the school. Further, Dr. Amuso testified that as part of Mrs. Volpi's duties as Coordinator it was necessary for her to occasionally inspect computers. The images in question here were discovered from the main screen of Defendants computer. Prior to Mrs. Volpi's discovery of the pictures, she had sent out a notice to all employees to remove their personal computers from the school due to the virus. Officer Evans personally observed

> the three pictures that depicted persons who appeared to be juveniles engaging in various sexual acts. The search was reasonable both at its inception and in its scope. All this information together would lead to sufficient probable cause for a search warrant. Therefore, the search was legal.
>
> The defendant's Motion to Suppress Physical Evidence is DENIED.

Appx. C3-C4. In its post-trial opinion, the Court of Common Pleas elaborated:

> The defense also contends that this court erred in denying a separate pretrial motion to suppress the contents of the computer based upon the defendant's privacy interest in the computer. Searches and seizures by government employers or supervisors of employee workspaces are subject to Fourth Amendment restraints. Commonwealth v. Jackson, 809 A.2d 411 (Pa. Super. 2002); O'Connor v. Ortega, 480 U.S. 709 (1987). However, the Fourth Amendment does not prohibit the reasonable search of a government employee's work area for non-investigatory, work-related purposes. Ortega, 480 U.S. at 725-26. For example, in Ortega officials at a public hospital searched the office of a doctor who was under investigation for misconduct. Id. at 712. The hospital justified the searches as a standard work-related inventory search of the office. Id. at 713. The doctor contended that the search was improper because it was a search related to the investigation into the alleged misconduct. Id. Writing for the plurality, Justice O'Connor ruled that while searches for

investigatory purposes require "reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct," necessary searches for noninvestigatory, work-related purposes require no further justification. Id. at 726.[1] Thus, government employers may freely search employee workspaces if necessary for such mundane tasks as the retrieval of a certain file. Id.

---

[1] Concurring in the decision, Justice Scalia similarly reasoned that employer searches carrying out work-related purposes should be considered reasonable whether the employer is private or governmental. Ortega, 480 U.S. at 732, Scalia, J., concurring.

Here, Ms. Volpi's search of the defendant's computer involved just such a mundane task. Ms. Volpi's duties included maintaining the health of the computer network. To do so, she needed to access all the computers on the network to make sure none were contaminated with malicious software dangerous to the network. On the day of the search, the network had been attacked by a virus,[10] making Ms. Volpi's task all the more urgent and necessary. Although the objected-to search involved Mr. Lamana's personal computer, not a computer owned by the school district, Mr. Lamana rendered such a search reasonable

---

[10] This statement is contrary to the record; see note 5 ante.

> when, against district policy, he connected his computer to the network.[11] Although an "employee may avoid exposing personal belongings at work by simply leaving them at home," and even in the face of a personal request from Ms. Volpi to remove the computer, Mr. Lamana kept his pornography-laden computer in his classroom and connected to the network.[12] Id. at 725. In light of these facts, the defense contention that Ms. Volpi should have obtained a warrant is absurd. And because Ms. Volpi had a standing right to access the computer as part of her regular duties, she also needed no court approval to show the questionable files to the superintendent and police. Therefore, this court properly denied the motion to suppress.

Appx. B5-B7. The question was then raised again on appeal to the Superior Court of Pennsylvania, which ruled as follows:

> Both the Fourth Amendment of the United States Constitution and Article 1, Section 8 of the Pennsylvania Constitution guard against unreasonable searches and seizures.

---

[11] The record contains no evidence at all that the computer belonging to petitioner that was searched and seized on November 29 (on which the evidence was found that was used in evidence) was ever attached to the school district's network, although another computer of his (which is not the source of the evidence in this case) had been. See text following note 5 ante.

[12] See note 11 ante.

> Commonwealth v. Harris, 888 A.2d 862, 868 (Pa.Super. 2005), appeal denied, 593 Pa. 746, 931 A.2d 656 (2007). Moreover, these constitutional restrictions are applicable to government employers and supervisors. O'Connor v. Ortega, 480 U.S. 709, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987) (Opinion Announcing the Judgment of the Court); Commonwealth v. Jackson, 809 A.2d 411 (Pa.Super. 2002). However, the standards governing the actions of government employers and supervisors are different than those governing law enforcement officers, and should be reviewed "according to the dictates of reason and common sense." O'Connor v. Ortega, supra, 480 U.S. at 725, 107 S.Ct. at 1501, 94 L.Ed.2d at 728 (Opinion Announcing the Judgment of the Court) (citation omitted).
>
> Based on our review of the record in this case, and the arguments of the parties, we conclude that the trial court was correct in its conclusion that there was no basis upon which to suppress the evidence that had been seized by the police. Thus, we agree with the decision to affirm the judgment of sentence, and do so based upon the well reasoned opinion filed by the learned Judge Thomas G. Parisi.[2]
>
> ---
>
> [2] We further note that, unlike the situation in Commonwealth v. Jackson, 809 A.2d 411 (Pa. Super. 2002), relied upon by appellant, the police here did ultimately obtain a warrant prior to effecting the seizure of appellant's computer.

App. A4-A5, referring to App. B.

Finally, the Fourth Amendment issue was advanced as a question sought to be reviewed in the petition for allowance of appeal to the Pennsylvania Supreme Court ("Whether a Public Employee Has a Right to Privacy in the Data Stored in a Personal Computer Located at Work," Pet. All. App. at 3). Petitioner's "argument [was] premised[, inter alia,] upon the United States Supreme Court's case of O'Connor v. Ortega 480 U.S. 709 (1987) (plurality opinion) ...." Pet. All. App. at 11. The state's highest court denied the application. Appx. D.

REASONS FOR GRANTING THE WRIT

Petitioner, a public employee, was convicted on a single count under Pennsylvania law of possessing child pornography. The jury acquitted him on another count. The evidence used against him was discovered in a forensic search of his personal computer, seized under a warrant. The warrant was secured on the basis of information obtained during prior warrantless searches of that computer by his employer's IT director and by a police officer. Attempting to apply this Court's decisions, the state courts of Pennsylvania upheld the constitutionality of these searches. That body of law remains unsettled in ways this case would allow the Court to address.

The relatively simple facts of this case make it a suitable vehicle for the Court to address the important issues it has twice granted certiorari to resolve: How does the Fourth Amendment apply to a public employer's workplace search of an employee's private property or information, which in turn leads to a warrantless law enforcement search and a criminal prosecution?

This case presents the Court with a favorable opportunity to resolve important Fourth Amendment issues which for nearly 25 years have eluded efforts to clarify the rules governing workplace searches by public employers. The Court granted certiorari in O'Connor v. Ortega, 480 U.S. 709 (1987), to decide whether a public employee has "a reasonable expectation of privacy in his office, desk, and file cabinets at his place of work," and then, if so, "the appropriate Fourth Amendment standard for a search conducted by a public employer in areas in which a public employee is found to have a reasonable expectation of privacy." Id. 712. The result was a plurality opinion and a judgment supported by the addition of a separate concurrence, endorsing a different constitutional test on both issues. These important constitutional issues were thus left unsettled.

Soon after, the Court addressed the issue of urine and breath testing for entire classes of government employees. The Court held that such testing, even when performed for a purpose other than law

enforcement, constituted a search governed by the Fourth Amendment. National Treas. Employees Union v. Von Raab, 489 U.S. 656, 665 (1989) (testing of government employees); Skinner v. Railway Labor Exec. Ass'n, 489 U.S. 602 (1989) (railroad acting under compulsion of governmental regulation). By a 5-4 vote, the Court held such testing reasonable as to certain types of employees, but remanded for further consideration as to others.

Just recently, the Court tackled these questions again. It granted certiorari in City of Ontario v. Quon -- this time, to decide whether certain police officers, or their civilian correspondents, had a reasonable expectation of privacy in text messages sent to and from an official pager. 558 U.S. --, 130 S.Ct. 1011 (No. 08-1332, order granting certiorari, 2009). Again, the Court decided the case without resolving the issue. 560 U.S. --, 130 S.Ct. 2619, 2632-33 (June 17, 2010).

The employer's conduct alleged to constitute a search in that case included the unnecessary reading of the messages themselves. Nevertheless, the Court unanimously determined that the investigation, even if it was a "search," was reasonable under the O'Connor v. Ortega plurality's approach, because it was motivated by a legitimate work-related purpose (to determine why monthly usage of the pagers was excessive). The Court held the examination of the pagers was a reasonable way to accomplish that objective, even though less intrusive means were available

and even if disclosure of the texts to the City by its service provider violated the federal Stored Communications Act.[13] At the same time, the Court declared the employer's actions in Quon would constitute a reasonable search under Justice Scalia's test, because the employer's examination of the pagers "would be 'regarded as reasonable and normal in the private-employer context ....'" 130 S.Ct. at 2633.

The Court in Quon thus resolved neither the question whether the employees enjoyed a reasonable expectation of privacy in personal messages sent to and from government-owned electronic equipment nor the question of which test (the O'Connor plurality's or Justice Scalia's) applies to determine the reasonableness of government employers' searches. By granting certiorari in petitioner's case, the Court would have an opportunity to address related and equally important questions.

It is now utterly commonplace for public employees to use employer-issued computers, cell phones, and other electronic equipment as part of their jobs. It is also not uncommon for public employees to use privately owned electronic equipment for job-related purposes, and probably even more common for public employees to bring privately owned electronics -- including portable computer equipment -- to work with them, if only for personal reasons. Indeed, with the increasing prevalence and

---

[13] Justices Stevens and Scalia also filed concurrences.

popularity of "smart phones" and applications such as "Skype" on computers (allowing live video-phone conversations), any attempted distinction between "computers" and "telephonic communication devices" is increasingly meaningless.

In this case, petitioner, a high school teacher, brought two different personal computers into the school building, and kept them in his assigned classroom. The school district provided computers that were intended to be used in the classroom -- connected to the school's "intranet" and through that connection to the internet. Petitioner, however, connected at least one of his personally-owned computers to the school's internal computer network, by plugging an ethernet cable from the computer into a data port in the classroom wall (much like a telephone jack). In this way, the computer could not only access data on the school's "server" but also make a high speed connection to the internet.

Investigating a high level of internet traffic through a certain data port and seeking the source of past virus infections, the school district's IT director came to petitioner's classroom, on a day he and the students were not there. She powered up a personally owned computer that was present, although it was not connected to the network at that time. (This was not the same computer as the one the IT director had observed connected to the port in petitioner's classroom and thus to the school's network more than three weeks earlier.) After turning this

computer on, she entered a command to display the computer's file structure. Observing a directory (folder) oddly named "shit," she proceeded to open the folder to see what kind of files it contained. At that point she noticed sexually explicit names of files, including some suggesting involvement of children. She opened and observed the contents of several of these before shutting off the computer and taking it to the IT office. There, the IT director displayed these same files to the Superintendent of Schools, who called the police.

After the responding police officer was told what the school officials had seen, he had them power up the computer and show him the offending files. Only after viewing several himself did he then leave to get a warrant.

Petitioner's motion to suppress was denied. At trial, the jury was allowed to hear not only the testimony of the police forensic expert who examined petitioner's computer after it was seized under the warrant, but also the testimony of the IT director about what she saw when she opened several of the files, as well as the testimony of the police officer about what he saw when the files were displayed to him prior to the warrant's being obtained. The denial of the motion to suppress was erroneous as to all three of these types of evidence, albeit for somewhat different reasons that this Court can and should explore after granting certiorari.

The evidence directly supporting the Commonwealth's case was seized under the warrant. The

validity of the warrant was not challenged in the motion to suppress, except insofar as the warrant was derived from the prior warrantless examination of petitioner's computer by the school district officials and the police officer. Because the evidence seized on the authority of the warrant was obtained as a result of the initial searches, and not through a "genuinely independent source," Murray v. United States, 487 U.S. 533, 543 (1988), it is not seriously disputable that this evidence should have been suppressed if the prior searches were unlawful.

The Pennsylvania courts in this case upheld the prior, warrantless searches of petitioner's computer on the basis of this Court's public employer work-place search cases. The state appellate court adopted the trial court's opinion. That ruling examined the initial search of the computer by Ms. Volpi, the IT director, and disregarded the intervening warrantless police search, as well as the examination of the suspect files by the Superintendent. Without discussing the separate concurrence that was necessary to this Court's decision, the trial court purported to apply the plurality decision in O'Connor v. Ortega. While the search might indeed have satisfied the test proposed by Justice Scalia (although this is by no means certain or conceded), the state courts here misapplied the plurality opinion. Certiorari should be granted to explore the correct analysis for the benefit of the lower courts.

a. Expectation of privacy

First, the Court can and should squarely hold that public employees enjoy a "legitimate expectation of privacy" in the contents of any privately-owned computer, cell phone, or other personal computing or communication device that the employee brings to work. See O'Connor v. Ortega, 480 U.S. at 719 (plurality), 730 (concurrence) (filing cabinets and desk at work); Mancusi v. DeForte, 392 U.S. 364 (1968) (same; private employer)[14]; see generally Kyllo v. United States, 533 U.S. 27, 33-34 (2001) (discussing definition of Fourth Amendment "search"). Such electronic data are "papers" within the meaning of the Fourth Amendment, since they perform the same social and personal functions of communication and record-keeping as literal "papers" in 1791.[15] Whether or not "reasonable" in its justifi-

---

[14] This case does not present the question, potentially implicated but not decided in Quon, whether public employees enjoy a reasonable expectation of privacy in the personal data they are authorized to transmit through or store on government-owned and -supplied communication equipment.

[15] See Peter Goldberger, Consent, Expectations of Privacy, and the Meaning of "Searches" in the Fourth Amendment, 75 J.Crim.L. & Crimin. 319, 342 (1984). If the Framers did not intend special protection from searches for letters, books, files, and so forth because of the communicative and record-keeping functions, there would have been no reason to mention "papers" in the Amendment separately from "effects." Id. n.110.

cation in a particular case, governmental examination of private papers kept in either electronic or more tangible form surely "infringes an expectation of privacy that society is prepared to recognize as reasonable," Skinner, 489 U.S. at 616, and thus constitutes a "search."

That legitimate societal expectation is not diminished because the devices used to create, transmit and store those electronic "papers" are kept, with or without the employer's permission, at work. It also should not depend on whether the employee is required or expected to use those devices, in part, for work-related functions. The expectation remains reasonable even when the computer or other electronic device is left in the workplace, a locked and unused classroom, over a long holiday weekend. Petitioner's apparent failure to password-protect the computer should also be immaterial. Nor would the expectation be lost simply because the computer may have been connected, at one time, to the employer's network,[16] at least in a case such as this where the computer was not so connected at the time of the search or when it was seized.[17]

---

[16] Indeed, there was no direct evidence that this computer ever was connected to the district's network, and probably not even a sufficient basis for an inference to that effect. See note 11 ante.

[17] Indeed, at the time of the search and seizure of petitioner's computer, the nearest network port had been disabled for some ten days. See p. 6 ante.

Whether the ensuing search was "reasonable" and thus constitutional is a separate and subsequent question, but the Court should recognize that examination of the files stored in petitioner's computer, even when that computer was left at the workplace of a public employee, was at least a "search" within the meaning of the Fourth Amendment.

b. What is the correct reasonableness test?

Under Justice Scalia's test, a public employer's examination of an employee's personal computer would surely be regarded as a search, but that search could be held reasonable if its purpose was "to retrieve work-related materials or to investigate violations of workplace rules -- searches of the sort that are regarded as reasonable and normal in the private-employer context." O'Connor, 480 U.S. at 732. Justice Scalia announced his adherence to this test in his separate concurrence in Quon. 130 S.Ct. at 2634. Even so, however, he "join[ed] the Court's opinion," id., not just its result, on the issue of whether the search in that case was reasonable. In other words, Quon was not a case presenting circumstances in which the Court might be forced to choose one test from O'Connor over the other. This case, on the other hand does arguably present such circumstances.

When the school district's IT director, Ms. Volpi, undertook her examination of petitioner's computer on November 29, she undoubtedly believed she was "investigat[ing potential] violations of workplace

rules" against connecting a personal computer to the district's network, particularly if loaded with file-sharing software. If this purpose alone suffices to render the search reasonable, then it met Justice Scalia's test. In his concurring opinions on this subject, Justice Scalia has been silent on the question of scope -- whether a search that eventually uncovers evidence of a crime, to be held reasonable, must have continued to be conducted solely for that work-related purpose throughout.

Justice Scalia has criticized the plurality's test as "standardless and unsupported," Quon, 130 S.Ct. at 2634, referencing O'Connor, 480 U.S. at 729-30 (calling standard "so devoid of content that it produces rather than eliminates uncertainty"). Yet it is not apparent to what authoritative source one might look to determine whether it would be "regarded as reasonable and normal in the private-employer context" for a private employer's IT director to do what Volpi did here. After initiating a search of an employee's computer for evidence of having been improperly connected to the employer's network, would it be "reasonable and normal" for the private IT director to open a folder labeled "shit" just to see what was in it? Then, upon seeing sexually suggestive file names, would it be "reasonable and normal" to open some of those files -- before calling the police -- to assess whether they might, as their names might make it seem, constitute child pornography?

Volpi never testified (in words or substance) that in doing so, she believed she was continuing "to

investigate violations of workplace rules." (The prosecutor never asked this question.) Purpose is subjective; does the absence of this evidence invalidate the search? See City of Indianapolis v. Edmond, 531 U.S. 32, 45-46 (2000) (distinguishing law enforcement searches from "special needs" and "programmatic" searches, as to relevance of subjective purpose). Does the search fail the test of reasonableness if at any point it proceeds further on the basis of mere curiosity, as may have occurred here (for all the record shows) when Volpi opened the folder labeled "shit," because she deemed its name "kind of inappropriate"? Although there was no such testimony here, is an employer objectively entitled to be concerned that an employee appears to be committing a possessory crime in the workplace, even if the contraband is in a "closed container" (here, a computer file)? Does the nature of the suspected offense matter? In what way? If so, then under Justice Scalia's test, the IT director's search might be held reasonable.

Under the O'Connor plurality's test, on the other hand, as applied there and as an alternative basis for the holding in Quon,[18] when a search is

---

[18] While the O'Connor plurality's test was applied by a seven-justice majority in Quon, Justice Kennedy's opinion for the Court repeatedly describes the majority's rationale as a mere application of the plurality test, rather than as the adoption of that test as a correct constitutional rule. 130 S.Ct. at 2630-33. Instead, the majority notes "that the search 'would be regarded as reasonable and normal in the

conducted "for a 'noninvestigatory, work-related purpos[e]' or for the 'the investigatio[n] of work-related misconduct,'" a Court should look to the "special needs of the [particular governmental] work-place," and ask whether the employer's warrantless search was "justified at its inception and if the measures adopted [were] reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search." Quon, 130 S.Ct. at 2630 (brackets original; some internal quotation marks omitted).

Under the O'Connor plurality test, Volpi's search was invalid, and the Pennsylvania courts clearly erred in holding otherwise. When she first powered up petitioner's computer on November 29 she mistakenly thought it was the same one she had seen attached to the school's network and running file-sharing software on November 2, when in fact it was an entirely different machine.[19] (This error, of

_____(cont'd)

private-employer context' and would satisfy the approach of Justice Scalia's concurrence" as well. Id. 2633.

[19] Apparently, when Volpi first turned the computer on, she was under the mistaken impression that it was the same computer she had observed in the classroom on November 2 and discussed with petitioner at that time. Tr.(5/6/08), at 40 ("I wanted to see if the virus was still on that machine and to see if Kazaa [the file-sharing program] was still on that machine."). She did eventually recognize that this was not the same machine, and in fact she had never seen it attached to the network. Id. 78.

course, must be considered a significant factor in deciding whether the search would still be "reasonable.") She then observed and opened the computer folder labeled "shit." In doing so, Volpi was no longer pursuing the investigation that arguably justified powering up petitioner's personal computer in the first instance (even though it was not then connected to the school's network). She was not looking in that folder to see whether the computer showed evidence of having been so connected or was the source of the repeated virus infections.[20]

Instead, seeing the oddly named folder, Volpi undertook the paradigmatic search that was "excessively intrusive in light of the circumstances giving rise" to the initial intrusion. Her inspection of the computer's contents took a new direction, motivated either by simple curiosity or by an entirely new and different investigative purpose. In either case, it would not satisfy the plurality test.

Thus, granting the writ of certiorari in this case may provide an opportunity, which the Court has heretofore not faced, of examining a record on which the search might be found reasonable under one test expounded in O'Connor v. Ortega, but not under the other.

---

[20] Volpi never said, for example, that she was looking in the folder for evidence of a file sharing program, and whether such software was recently used.

c. Initial warrantless police examination.

In addition to the opportunity to address the unresolved O'Connor issue in a setting where it matters, there is a final problem with the analysis of the Pennsylvania courts below, and thus with their judgment, which warrants this Court's review. The courts below never addressed the significance, under the Fourth Amendment (or otherwise) of the fact that the search warrant for petitioner's computer was not based on what the school district officials told Officer Evans, but rather on the basis of what he himself saw when they powered up petitioner's computer again for him upon his initial arrival at the high school.[21] It is not clear whether the Pennsylvania courts simply overlooked this question, or whether they assumed that the district had authority to consent to a police search of petitioner's computer.

Because the suspicious evidence was in computer files, and the computer had been shut down before the police were called, the school officials could not and did not merely show the police what they had already discovered in a justified workplace search

---

[21] What it is that the superintendent and Ms. Volpi told Officer Evans, either over the phone or when he arrived, before he had them allow him to search the computer again himself, is not disclosed in this record. Thus, there is no basis to say whether probable cause existed at that point already. As a result, the pre-warrant search problem cannot be avoided on the basis of "inevitable discovery" or the like.

(even if that prior search were to be held reasonable and justified). Instead, it was necessary to conduct a new and further search of the computer's stored files -- this one, directed by Officer Evans -- to show him what he wanted to see and not just hear about. Cf. Walter v. United States, 447 U.S. 649 (1980) (examination of obscene films by FBI prior to obtaining warrant was illegal search, despite prior lawful opening of package by shipper).

District officials had neither actual nor apparent authority to consent to a police search of petitioner's personal computer that he had left over the holiday weekend in his locked classroom. See generally Georgia v. Randolph, 547 U.S. 103 (2006) (surveying issues of authority and scope of consent); United States v. Matlock, 415 U.S. 164 (1974) (consent from co-habitant of sublessor of room in rented house); Frazier v. Cupp, 394 U.S. 731, 740 (1969) (joint user of duffel bag). They lacked "common authority" over petitioner's personal computer. Illinois v. Rodriguez, 497 U.S. 177, 181-82 (1990) (former co-habitant, who still possessed key and sometimes spent the night, lacked authority to consent to search).

Once the police were called in, this was no longer, contrary to what the Pennsylvania courts seemed to think, a workplace search situation. See Ferguson v. City of Charleston, 532 U.S. 67 (2001) (governmental search cannot be justified under "special needs" doctrine, regardless of motive, where criminal law enforcement involvement is pervasive).

Rather, the initial warrantless search by Officer Evans, after being called by the school officials but before seeking a warrant, was itself a violation of the Fourth Amendment of which the later-obtained warrant (which yielded the evidence underlying the conviction) was a tainted fruit. In this final way as well, the courts below failed to follow this Court's precedent, raising interrelated constitutional issues worthy of this Court's review.

For all these reasons, the petition for a writ of certiorari should be granted.

CONCLUSION

The Court should grant this petition and issue a writ of certiorari to the Superior Court of Pennsylvania to review the judgment and memorandum affirming petitioner Lamana's conviction and sentence. At the very least, the Court should grant certiorari and remand to the Pennsylvania courts for further consideration in light of the majority opinion in City of Ontario v. Quon, 560 U.S. --, 130 S.Ct. 2619 (2010).

Respectfully submitted,

PETER GOLDBERGER
Counsel of Record
PAMELA A. WILK
50 Rittenhouse Pl.
Ardmore, PA 19003
(610) 649-8200

MARC NEFF
13th Floor
1818 Market Street
Philadelphia, PA 19103
(215) 563-9800

Attorneys for Petitioner

August 25, 2010

APPENDIX A

J. A22025/09
NON-PRECEDENTIAL DECISION –
SEE SUPERIOR COURT I.O.P. 65.37

IN THE
SUPERIOR COURT OF PENNSYLVANIA
NO. 1924 MDA 2008

COMMONWEALTH OF PENNSYLVANIA,

Appellee

v.

PETER JOHN LAMANA,

Appellant

Appeal from the Judgment of Sentence
entered October 14, 2008,
In the Court of Common Pleas of Berks County,
Criminal, No. CP-06-CR-0004172-2005

BEFORE: GANTMAN, FREEDBERG, JJ., and McEWEN, P.J.E.

MEMORANDUM: FILED: November 23, 2009

Appellant, Peter John Lamana, appeals from the judgment of sentence to serve a term of imprisonment of from four months to twenty-three months, a sentence imposed after a jury convicted him of one count of sexual abuse of children-possession of child pornography.[1] We affirm.

The trial court has provided the following summary of the relevant facts underlying this appeal:

> The charges against Mr. Lamana arose from the discovery of child pornography on his personal computer while a teacher at Boyertown High School. In October and November of 2004, Karla

[1] *See:* 18 Pa.C.S. § 6312(d).

Volpi, the Boyertown School District IT Manager, tracked a number of incidents of unusual traffic on the school district computer network. Because it was her job to maintain the network the traffic concerned Ms. Volpi. In addition, on November 2, 2004, an incident of unusual traffic coincided with a massive computer virus attack on the network. After this incident, Ms. Volpi found the source of the unusual traffic: Mr. Lamana's personal computer, which he had installed in his classroom and connected to the school network. Ms. Volpi turned off the network port to which Mr. Lamana had connected his computer, citing the district policy against personal computers on the network, and asked the defendant to take his computer home. However, she soon acquiesced to Mr. Lamana's plea for a short-term reprieve and reopened the port to Mr. Lamana's computer.

On November 29, 2004, a virus again attacked the school district network. Ms. Volpi decided to investigate Mr. Lamana's computer to see if it was the source of the virus. Ms. Volpi entered the defendant's classroom, which had been locked for a school holiday, and turned on the defendant's personal computer. Almost immediately after turning on the computer, Ms. Volpi found a folder named "shit." Inside the folder she found files with various sexual titles. She noted files with titles indicating children and sex acts. She opened some of these files, finding images and video of children participating in sex acts. [At trial, the defense stipulated that images and video on the defendant's computer constituted child pornography]. She noted that these files had last been accessed on November 24, 2004. Later that day [November 29], she reopened some files to show the images to then-superintendent Dr.

> Charles Amuso and the police. Before Mr. Lamana could again access the computer, the police executed a warrant for its seizure. Its contents became the basis of the charges Mr. Lamana faced at trial.

Trial Court Opinion, February 2, 2009, pp. 1-2.

Prior to trial appellant filed, *inter alia*, a motion to suppress the seizure of his computer, which was denied. The case proceeded to a jury trial on two counts of sexual abuse of children, as defined at 18 Pa.C.S. § 6312(d), namely,

> Intentionally view[ingJ or knowingly possess[ing] or control[ling] any ... computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such act commits an offense.

At the conclusion of the trial the jury found appellant guilty of one count of sexual abuse of children. Following the imposition of sentence, appellant filed this appeal.

Appellant, in the brief submitted in support of this appeal, argues that the trial court erred in denying his motion to suppress because the warrantless search of his computer by school officials and police violated his constitutionally protected rights against an illegal search and seizure. The principles governing our review of this argument are well established.

> Our standard of review of a denial of suppression is whether the record supports the trial court's factual findings and whether the legal conclusions drawn therefrom are free from error. Our scope of review is limited; we may consider only the evidence of the prosecution and so much of the evidence for the defense as remains uncontra–dicted when read in the context of the record as a

> whole. Where the record supports the findings of the suppression court, we are bound by those facts and may reverse only if the court erred in reaching its legal conclusions based upon the facts.

Commonwealth v. A. Brown, 924 A.2d 1283, 1286 (Pa.Super. 2007) (citation omitted). Both the Fourth Amendment of the United States Constitution and Article 1, Section 8 of the Pennsylvania Constitution guard against unreasonable searches and seizures. *Commonwealth v. Harris,* 888 A.2d 862, 868 (Pa.Super. 2005), *appeal denied,* 593 Pa. 746, 931 A.2d 656 (2007). Moreover, these constitutional restrictions are applicable to government employers and supervisors. *O'Connor v. Ortega,* 480 U.S. 709, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987) (Opinion Announcing the Judgment of the Court); *Commonwealth v. Jackson,* 809 A.2d 411 (Pa.Super. 2002). However, the standards governing the actions of government employers and supervisors are different than those governing law enforcement officers, and should be reviewed "according to the dictates of reason and common sense." *O'Connor v. Ortega, supra,* 480 U.S. at 725, 107 S.Ct. at 1501, 94 L.Ed.2d at 728 (Opinion Announcing the Judgment of the Court) (citation omitted).

Based on our review of the record in this case, and the arguments of the parties, we conclude that the trial court was correct in its conclusion that there was no basis upon which to suppress the evidence that had been seized by the police. Thus, we agree with the decision to affirm the judgment of sentence, and do so based upon the well reasoned opinion filed by the learned Judge Thomas G.

Parisi.[2]

Judgment of sentence affirmed.

Judgment Entered.
/s/ [illegible]
Deputy Prothonotary

Date: November 23, 2009

---

[2] We further note that, unlike the situation in *Commonwealth v. Jackson,* 809 A.2d 411 (Pa.Super. 2002), relied upon by appellant, the police here did ultimately obtain a warrant prior to effecting the seizure of appellant's computer.

Appx. B

2009 WL 1514617, 7 Pa. D. & C. 5th 225
Court of Common Pleas of Pennsylvania,
Berks County

Commonwealth
v.
Lamana

No. CP-06-CR-4172-2005.

February 2, 2009

Seth Boer, trial attorney for Commonwealth.
Adrian Shchuka, appeal attorney for Commonwealth.
Marc Neff, for defendant.

PARISI, *J.*

On May 8, 2008, a jury found Mr. Lamana guilty of one count of possession of child pornography,[1] acquitting him of another count. On October 14, 2008, the defendant received a sentence of four to 23 months of incarceration followed by five years of probation. He filed a timely appeal on October 28, 2008. In the present appeal, Peter Lamana challenges the denial of his pretrial motions, specifically motions seeking remedies for the alleged destruction of evidence and a motion to suppress evidence.

The charges against Mr. Lamana arose from the discovery of child pornography on his personal computer while a teacher at Boyertown High School. In October and November of 2004, Karla Volpi, the Boyertown School District IT manager, tracked a

[1] Sexual abuse of children, 18 Pa.C.S. §6312(d).

number of incidents of unusual traffic on the school district computer network. Because it was her job to maintain the network, the traffic concerned Ms. Volpi. In addition, on November 2, 2004, an incident of unusual traffic coincided with a massive computer virus attack on the network. After this incident, Ms. Volpi found the source of the unusual traffic: Mr. Lamana's personal computer, which he had installed in his classroom and connected to the school network. Ms. Volpi turned off the network port to which Mr. Lamana had connected his computer, citing the district policy against personal computers on the network, and asked the defendant to take his computer home. However, she soon acquiesced to Mr. Lamana's plea for a short-term reprieve and reopened the port to Mr. Lamana's computer.

On November 29, 2004, a virus again attacked the school district network. Ms. Volpi decided to investigate Mr. Lamana's computer to see if it was the source of the virus. Ms. Volpi entered the defendant's classroom, which had been locked for a school holiday, and turned on the defendant's personal computer. Almost immediately after turning on the computer, Ms. Volpi found a folder named "shit." Inside the folder she found files with various sexual titles. She noted files with titles indicating children and sex acts. She opened some of these files, finding images and video of children participating in sex acts.[2] She noted that these files had last been accessed on November 24, 2004. Later that day, she reopened some files to show the images to then-superintendant Dr. Amuso and the police. Before Mr. Lamana could again access the computer,

---

[2] At trial, the defense stipulated that images and video on the defendant's computer constituted child pornography.

the police executed a warrant for its seizure. Its contents became the basis of the charges Mr. Lamana faced at trial.

Ms. Volpi's opening of the child pornography files became the basis for the first two pretrial motions contested in the present appeal. Files such as the ones opened by Ms. Volpi track the last time they were opened and viewed. Each time a file is opened, the data is altered to reflect the most recent use, and users can easily see when the file was last opened. Police investigating computer crimes typically create a forensic image of the contents of a computer, preserving the data exactly as it was when they obtained the computer. This allows them to open and close files without changing any data about the last time a file was opened prior to seizure. Both the prosecution and the defense can then utilize the forensic image, assured that the data they access remains as it was when last controlled by the defendant.

Here, because Ms. Volpi opened and viewed the child pornography files, neither the prosecution nor the defense could access data about the last time the files were viewed when Mr. Lamana still had access to the computer. Each time she opened the pornographic files, the data about last use changed to reflect her most recent viewing. By the time the police seized the computer, all of the child pornographic files from the computer reflected a last use on November 29, 2004, at the time Ms. Volpi had the computer under her control. Although Ms. Volpi testified at trial that the last time the files were opened prior to her discovery was November 24, 2004, the parties had no way to independently verify this testimony because the data was lost.

Because of the altering of this potentially exculpatory evidence, the defense moved for drastic

remedies-dismissal of the charges or preclusion of all testimony concerning the contents of the computer. This court denied these motions after a pretrial hearing on the matter. The defendant now appeals the denial of these motions, contending that he was denied due process of law. However, the minor alteration of the evidence, made prior to seizure, not by the police, and without any bad faith, could not justify the granting of the defendant's motions.

To justify corrective sanctions for lost or destroyed evidence, such as the suppression sought by the defendant here, the defendant must demonstrate that the police acted in bad faith in losing or destroying the evidence. *Commonwealth v. Small*, 559 Pa. 423, 441, 741 A.2d 666, 676 (1999), citing *Arizona v. Youngblood*, 488 U.S. 51 (1988). Here the police did not commit the alleged destruction of the evidence. In addition, Ms. Volpi's conduct did not evidence an effort to obscure the facts or railroad Mr. Lamana into a conviction or any other questionable motives suggesting bad faith. Because the date was altered prior to the police seizure, neither party was able to examine the lost data; everything available to the prosecution was available to the defense. In addition, the defense was able at trial to fully explore the loss of the data to suggest that the defendant was unaware of the contents of his computer. Finally, the contraband files remained otherwise intact-the defense even stipulated that they were child pornography.[3]

---

[3] The defense has argued that the unusual case of *Commonwealth v. Deans*, 530 Pa. 514, 610 A.2d 32 (1992), entitles Mr. Lamana to relief. In *Deans*, the Supreme Court of Pennsylvania ruled that a defendant's due process rights were violated where the police lost an allegedly forged lottery ticket prior to the filing of a forgery charge. *Id.* However, in *Deans* the lost evidence

Therefore, the alteration of the last-opened date in the files did not deny Mr. Lamana of due process of law and no corrective sanctions were warranted.

The defense also contends that this court erred in denying a separate pretrial motion to suppress the contents of the computer based upon the defendant's privacy interest in the computer. Searches and seizures by government employers or supervisors of employee workspaces are subject to Fourth Amendment restraints. *Commonwealth v. Jackson*, 809 A.2d 411 (Pa. Super. 2002); *O'Connor v. Ortega*, 480 U.S. 709 (1987). However, the Fourth Amendment does not prohibit the reasonable search of a government employee's work area for non-investigatory, work-related purposes. *Ortega*, 480 U.S. at 725-26. For example, in *Ortega* officials at a public hospital searched the office of a doctor who was under investigation for misconduct. *Id.* at 712. The hospital justified the searches as a standard work-related inventory search of the office. *Id.* at 713. The doctor contended that the search was improper because it was a search related to the investigation into the alleged misconduct. *Id.* Writing for the plurality, Justice O'Connor ruled that while searches for investigatory purposes require "reasonable grounds for suspecting that the

---

constituted the primary evidence of the crime and had been fully available to the prosecution, but not the defense, for expert evaluation. *Id.* at 517, 610 A.2d at 34. Here, the lost evidence was not the primary evidence of the crimes charged, and it was not available to either side, except in the form of Ms. Volpi's testimony. And Ms. Volpi testified only to what she saw - she did not provide expert opinion explaining how her observation of the last-viewed date implicated the defendant. Therefore, *Deans* does not apply to the case at hand.

search will turn up evidence that the employee is guilty of work-related misconduct," necessary searches for noninvestigatory, work-related purposes require no further justification. *Id.* at 726.[4] Thus, government employers may freely search employee workspaces if necessary for such mundane tasks as the retrieval of a certain file. *Id.*

Here, Ms. Volpi's search of the defendant's computer involved just such a mundane task. Ms. Volpi's duties included maintaining the health of the computer network. To do so, she needed to access all the computers on the network to make sure none were contaminated with malicious software dangerous to the network. On the day of the search, the network had been attacked by a virus, making Ms. Volpi's task all the more urgent and necessary. Although the objected-to search involved Mr. Lamana's personal computer, not a computer owned by the school district, Mr. Lamana rendered such a search reasonable when, against district policy, he connected his computer to the network. Although an "employee may avoid exposing personal belongings at work by simply leaving them at home," and even in the face of a personal request from Ms. Volpi to remove the computer, Mr. Lamana kept his pornography-laden computer in his classroom and connected to the network. *Id.* at 725. In light of these facts, the defense contention that Ms. Volpi should have obtained a warrant is absurd. And because Ms. Volpi had a standing right to access the computer as part of her regular duties, she also needed no court

---

[4] Concurring in the decision, Justice Scalia similarly reasoned that employer searches carrying out work-related purposes should be considered reasonable whether the employer is private or governmental. *Ortega*, 480 U.S. at 732, Scalia, J., concurring.

approval to show the questionable files to the superintendent and police. Therefore, this court properly denied the motion to suppress.

For the foregoing reasons, it is respectfully requested that the defendant's appeal be denied.

Appx. C

IN THE COURT OF COMMON PLEAS
OF BERKS COUNTY, PENNSYLVANIA
CRIMINAL DIVISION

No. 05-4172

COMMONWEALTH OF PENNSYLVANIA
vs.
PETER LAMANA,
Defendant

Marc Neff, Esquire
Attorney for the Defendant
Craig Scheetz, Esquire, Assistant District Attorney
Attorney for the Commonwealth

CLERK OF COURTS
'07 JAN 10 P4:55
BERKS COUNTY

FINDINGS OF FACT AND CONCLUSIONS OF LAW IN DISPOSITION OF DEFENDANT'S OMNIBUS MOTION FOR PRETRIAL RELIEF

Defendant is charged with two counts of Sexual Abuse of Children (Child Pornography). Defendant filed his Omnibus Pre-trial Motion on April 6, 2006, which included a Motion to Suppress Physical Evidence and Motion to Suppress Statements. The Pre-trial hearing was held on August 21, 2006.

FINDINGS OF FACT

On November 29, 2004, Officer Robert Evans, of the Colebrookdale District Police Department, received a call from Boyertown High School. Following the call, Officer Evans met with Dr. Amuso, Superintendent of the School, and Mrs. Karla Volpi, the Coordinator of Instructional Technology. Dr. Amuso and Mrs. Volpi expressed

concern regarding recent computer related activity at the school and directed Officer Evans to classroom 803 where the activity was occurring. Mrs. Volpi advised Officer Evans that she came to discover the images because of her work in connection with a computer virus that had recently affected the school.

Once in the room, Mrs. Volpi turned on a Compaq Presario computer, belonging to the Defendant, and clicked on an icon from the main screen revealing pornographic photographs. Officer Evans observed three pictures that depicted persons, who appeared to be juveniles, engaging in various sexual acts.

Based on the above, Officer Evans secured the room and obtained a search warrant for the computer. Officer Evans executed the search warrant that same day. Items seized included the computer tower and other computer related devices and disks from the desk on which the computer was located.

Dr. Amuso testified that Mrs. Volpi is in charge of the efficient operation of the electronic technology of the school district; computers, local area network, Internet connections and purchasing and advising to purchase all the computer equipment of he district. He further testified that as part of her duties as Coordinator it was necessary for her to occasionally inspect computers. Prior to Mrs. Volpi's discovery of the pictures, she had sent out a notice to all employees to remove their personal computers from the school due to the virus that had recently occurred. The school issued its own Compaq computers for school use.

CONCLUSIONS OF LAW

Where a motion to suppress has been filed, the burden is on the Commonwealth to establish by a

preponderance of the evidence that the challenged evidence is admissible. *Commonwealth v. Denmark*, 800 A.2d 952 (Pa. Super. 2002). The general rule is that a search warrant is required before police may conduct any search. The scope of a lawful search pursuant to a warrant requires that there be probable cause for the object of the search and the places where it is believed to be found. *Commonwealth v. Kiessling*, 552 A.2d 270, 272 (Pa. Super. 1998).

To determine if a warrant is supported by probable cause the magistrate cannot look outside the four corners of the affidavit. *Commonwealth v. Coleman*, 830 A.2d 554, 560 (Pa. 2003). The affidavit must contain sufficient information to establish probable cause at the time the warrant is authorized. *Id.*

Searches and seizures by government employers or supervisors of the private property of their employees are subject to Fourth Amendment restraints. *Commonwealth v. Jackson*, 809 A.2d 411, 2002 Pa. Super 311; *O'Connor v. Ortega*, 480 U.S. 709, 107 S.Ct. 1492. However, the operational realities of the workplace may make *some* public employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. 480 U.S. at 710. Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis. *Id.*

In determining the appropriate standard for a search conducted by a public employer in areas in which an employee has a reasonable expectation of privacy, what is a reasonable search depends on the context within which the search takes place, and requires balancing the employee's legitimate

expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace. *Id.* Intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this standard, both the inception and the scope of the intrusion must be reasonable. *Id.*

Here, the initial discovery by Mrs. Volpi was reasonable and there was sufficient probable cause to obtain a search warrant. Mrs. Volpi advised Officer Evans that she came to discover the pornographic images on the Defendant's computer because of her work in connection with a computer virus that has recently affected the school. Further, Dr. Amuso testified that as part of Mrs. Volpi's duties as Coordinator it was necessary for her to occasionally inspect computers. The images in question here were discovered from the main screen of Defendants computer. Prior to Mrs. Volpi's discovery of the pictures, she had sent out a notice to all employees to remove their personal computers from the school due to the virus. Officer Evans personally observed the three pictures that depicted persons who appeared to be juveniles engaging in various sexual acts. The search was reasonable both at its inception and in its scope. All this information together would lead to sufficient probable cause for a search warrant. Therefore, the search was legal.

The defendant's Motion to Suppress Physical Evidence is DENIED.

Motion to Suppress Statements

The defendant also makes a motion to suppress his statements alleging violations of his

Constitutional rights. For *Miranda* to apply, the defendant must be subject to at least a custodial interrogation. Custodial interrogation implies questioning initiated by police after a defendant "has been taken into custody or otherwise deprived of his freedom of action in any significant way." *Commonwealth v. Heggins*, 809 A.2d 908, 914 (Pa. Super. 2002) quoting *Commonwealth v. McGrath*, 470 A.2d 487, 491-492 (Pa. 1983). "Interrogation is defined as police conduct calculated to, expected to, or likely to evoke emission." *Id.* quoting *Commonwealth v. McGrath*, 725 A.2d 196, 200 (Pa. Super. 1999).

Here, the Defendant made statements to Boyertown school personnel. He made no statements to police. Therefore, Defendant's request to suppress statements is MOOT.

ORDER OF COURT

AND NOW, January 12, 2007, after hearing held on the Defendant's Omnibus Motion for Pretrial Relief, it is **ORDERED** that the Defendant's Motion to Suppress Physical Evidence is DENIED. The Motion to Suppress Statements is MOOT.

BY THE COURT:
s/Thomas G. Parisi
THOMAS G. PARISI, J.

Appx. D

2010 WL 2106952

In the Supreme Court of Pennsylvania

Middle District

COMMONWEALTH OF PENNSYLVANIA,

Respondent

v.

PETER JOHN LAMANA, Petitioner

No. 975 MAL 2009

Petition for Allowance of Appeal

from the Order of the Superior Court

ORDER

PER CURIAM

AND NOW, this 27th day of May 2010, the Petition for Allowance of Appeal is denied.

TRUE & CORRECT COPY

ATTEST: May 27, 2010

s/Elizabeth E. Zisk

Elizabeth E. Zisk, Chief Clerk